

CISO MAG

beyond cybersecurity

Volume 1 | Issue 2 | September - October 2017



Fintech: Rooted in the Past, Borrowed from the Future

Understanding Trends and the
Cybersecurity Skills Gap

To CISOs With Love:
Endpoints are Dead

Cyber Insurance and
the Liability Paradox

Automation and Orchestration:
The Big Picture



**NO RULES
NO SIGNATURES
NO ASSUMPTIONS**

Powered by machine learning and AI algorithms, Darktrace's Enterprise Immune System detects emerging threats inside your network that no one else can find.

darktrace.com

“The clear leader in
anomaly detection”

451 Research



INDEX

- 06 BUZZ**
Cyber Insurance and the Liability Paradox

- 12 UNDER THE SPOTLIGHT**
An Interview with Tim Fitzgerald

- 17 VIEW POINT**
To CISOs with Love: Endpoints are Dead

- 22 COVER STORY**
Fintech: Rooted in the Past,
Borrowed from the Future

- 27 IN THE HOTSEAT**
High-Profile Appointments
in the Cybersecurity World

- 30 TABLETALK**
Few Minutes with Foo Siang-Tse

- 35 EVENT FOCUS**
A Curtain Raiser to Global CISO Forum

- 38 INDUSTRY SPEAKS**
In Discussion with Tobias Gondrom

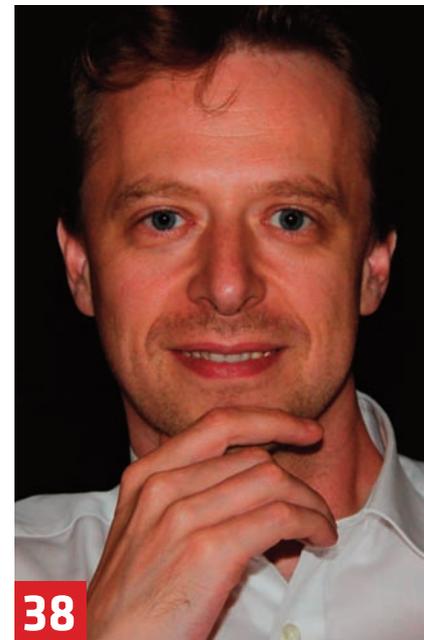
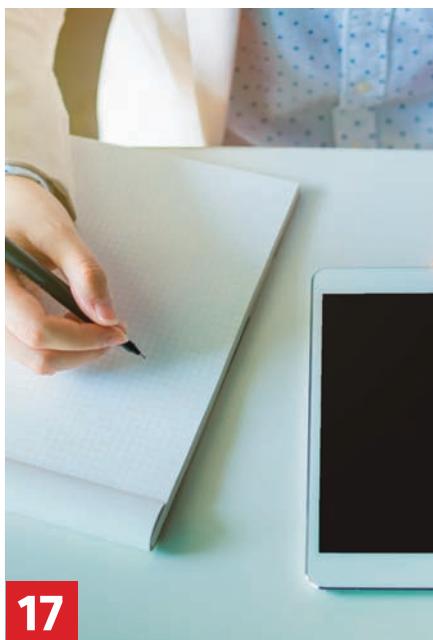
- 43 IN THE NEWS**
Top Stories from the Cybersecurity World

- 49 TECHTALK**
Automation and Orchestration: The Big
Picture

- 56 KICKSTARTERS**
Startups Making Waves in the
Cybersecurity World

- 62 KNOWLEDGE HUB**
Understanding Trends and the
Cybersecurity Skills Gap

- 74 COLLABORATIONS**
Famous Collaborations in the
Cybersecurity World





It may not be wrong to say that fintech has changed the way financial services are offered to consumers. It is a perfect option for the consumers, businesses, and financial institutions who in today's connected, on-demand world want to transact in a convenient, timely, secured, and efficient manner. The future may see financial transactions being made majorly through Bitcoins, Ethers, and other future cryptocurrencies.

Traditional banks have realized that fintech is the future; they are either running for cover or trying to stay relevant by embracing new technology solutions. The countries are also aware of the evolving fintech landscape and understand how crucial it is for economic growth. However, for fintech, a number of challenges lie ahead. In the cover story, we throw light on some of these key challenges which include lack of unilateral policies and standardizations and several cyber attack vectors.

In the Buzz section, we discuss cyber insurance, a key mitigation tool for businesses in an age where deepening dependence on technology is exposing them to greater cyber threats. Move on the Viewpoint section where our executive contributor Chris Roberts pens a candid open letter to CISOs, stripping away the hype surrounding endpoint protection.

For this issue, we interviewed three cybersecurity stalwarts – Tim Fitzgerald, CSO, Symantec; Foo Siang-Tse, Senior Managing Director, Quann; and Tobias Gondrom, CTO, Huawei. They talk about their journeys, evolving cybersecurity landscape, and challenges ahead, among many other things.

The magazine comprises a host of other informative features that look cybersecurity from an all-encompassing perspective – regulations, workforce development, partnerships, and much more.

Tell us what you think of this issue. If you have any suggestions, comments, or queries, please reach us at editorial@cisomag.com.

Jay Bavisi

Editor-in-Chief
jay@eccouncil.org

CISO MAG

beyond cybersecurity

Volume 1 | Issue 2
September - October 2017

Editorial

International Editor

Amber Pedroncelli
amber.pedroncelli@eccouncil.org

Senior Editor

Rahul Arora
rahul.arora@eccouncil.org

Feature Writer

Augustin Kurian
augustin.k@eccouncil.org

Content Writer

Sandip Acharyya
sandip.acharyya@eccouncil.org

Media and Design

Media Director

Saba Mohammad
saba.mohammad@eccouncil.org

Design Head and Visualizer

MSH Rabbani
rabbani@eccouncil.org

Designer

Surendra Bitti
surendra@eccouncil.org

Management

Executive Director

Apoorba Kumar*
apoorba@eccouncil.org

Senior Director, Compliance & Governance

Cherylann Vanderhede
cherylann@eccouncil.org

Marketing & Sales

General Manager

Meghana Vyas
meghana.vyas@eccouncil.org

Marketing Manager

Jinu Francis
jinu.francis@eccouncil.org

Sales Manager - India

Basant Das
basant.das@eccouncil.org

Sales Manager - North America

Jessica Johnson
jessica.johnson@eccouncil.org

Technology

Director of Technology

Raj Kumar Vishwakarma
rajkumar@eccouncil.org



CYBER INSURANCE AND THE LIABILITY PARADOX

Augustin Kurian



Addressing the gathering of CISOs at the 3rd Annual CISO Summit held in Mumbai, India, in July 2017, Sunil Varkey, CISO of Wipro Technologies, pointed out, “The role of CISOs is way more complex because they handle a domain called cybersecurity. CISOs pester the management to increase the cybersecurity spending. When asked by the management if higher spending would mean the organization would not be compromised, the CISOs often respond by saying, ‘I don’t know.’”

However, complexity often derives new solutions and one of them is cyber insurance. Cyber insurance is not a hot topic and has been around for over a decade and a half. It was designed to alleviate losses incurred from cyber attacks and is a key tool that plays crucial roles. According to the United States Department of Homeland Security, “A robust cybersecurity insurance market could help reduce the number of successful cyber attacks by: (1) promoting the adoption of preventative measures in return for more coverage; and (2) encouraging the implementation of best practices by basing premiums on an insured’s level of self-protection.”

Timetric, in its recent ‘Insight Report: Developments in Cyber insurance,’ concluded that the growing number of attacks have turned cyber insurance into a key mitigation tool. “Although cyber insurance does not replace the need for cybersecurity technology, it has the ability to complement cybersecurity standards through mitigating cyber risk.”

According to Allianz SE, organizations are paying roughly \$3.25 billion each year in annual premiums for cyber insurance. But

that number is small considering the cyber insurance market is expected to reach \$20 billion by 2025.

WHO NEEDS CYBER INSURANCE?

Everyone! Cybercriminals are not Robin Hood, they do not differentiate between a large company and a small company, and they will do what they do best—steal. While big corporations fortify themselves with several layers of protection, small businesses often underestimate the potential impact of cyber attacks. Many small business owners believe that hackers only attack high-profile organizations when the reality is just the opposite. In fact, nearly 90 percent of breaches occur in small businesses. A bigger concern is that



The role of CISOs is way more complex because they handle a domain called cybersecurity. CISOs pester the management to increase the cybersecurity spending. When asked by the management if higher spending would mean the organization would not be compromised, the CISOs often respond by saying, ‘I don’t know.’



nearly 60 percent of small businesses who face cyber attacks shut down within six months of the attack.

Because news coverage of attacks primarily focuses on big corporations, small businesses are unaware of the threat they face. "For small businesses, nothing is more important than protecting their livelihood. Cyber liability insurance is another tool they can use to prevent

financial disaster in the event of a malicious attack," stated Natalie Cooper, editor of BankingSense.com in a report from Cyber Insurance Guide.

THE MISMATCH

While cyber threats have drastically evolved from the time cyber insurance was first offered, the cyber insurance market hasn't. One of the

reasons is that the cyber insurance market is largely based on old-fashioned ideas about information security and what kind of coverage a breached company will actually need.

A study by Marsh and the UK Government in 2015 concluded that cyber insurance premiums are almost three times higher than commercial general liability policies.



TAKEAWAYS FOR CISOs

- ▶ Work with your organization’s risk management stakeholders to understand prospective or existing insurance policies. Understand what is explicitly covered, what is not, and how the policy could be defended in court
- ▶ Ensure that you are a part of the buying and renewal process
- ▶ Be a part of the underwriting process
- ▶ Communicate with insurers about prior breaches

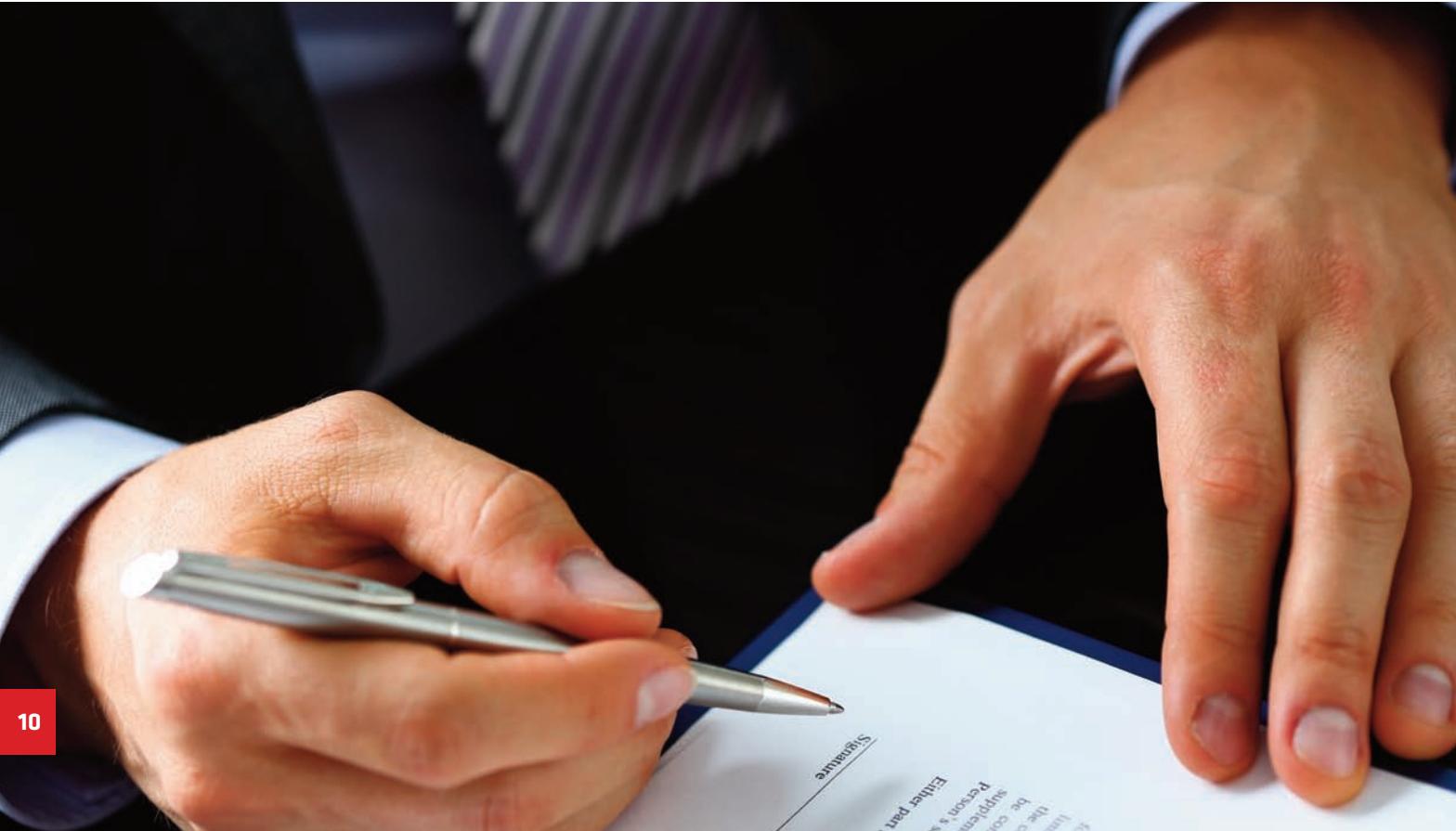
But even here, there has been a huge gap between the damage incurred and the breadth of policy coverage. For example, in 2014, when PF Chang’s, a U.S.-based dining restaurant chain, was hacked and credit card information of nearly 60,000 customers were leaked, Chubb cyber-insurance, the insurer, only covered the cost incurred for investigation of the data breach, legal advice, and the expenses for notifying authorities and customers.

PF Chang’s policy with Chubb stated that it would “address the full breadth of risks associated with doing business in today’s technology-dependent world,” but, PF Chang’s argued, much of the cost of having been breached was not, in fact, covered. Due to this discrepancy, PF Chang’s sued Chubb to recover an additional \$2 million the company was required to repay credit card companies whose details were stolen in the hack and subsequently used to

make fraudulent transactions. The suit was rejected by the court upon hearing the argument from Chubb that the policy signed by PF Chang’s did not cover any external contract or agreement the company held.

Perhaps if more companies find themselves in situations like PF Chang’s did, cyber insurance policies will be forced to evolve in accordance to the needs of the market. As it stands now, high premiums keep





cyber insurance out of reach for most medium and small businesses, but as insurance companies strive to beat their competition with better, more comprehensive policies, prices will fall too.

SOLUTION FOR THE PRESENT PERILS

The PF Chang's case is an example of a company not fully understanding its insurance policy, or at least, not fully understanding how that policy could be defended in court and leave them vulnerable. According to a report by JLT Re and JLT Specialty Limited, "Traditional P&C (property and casualty) products were not designed to protect against today's fast-moving cyber risk landscape. And there are now growing fears that future losses may bring

unanticipated accumulations due to potential 'silent' exposures." Silent cyber risks are things like "(re)insurers' potential exposure to cyber losses within P&C products where no explicit exclusions are included. And even where exclusions are included, gaps can emerge in the event of unforeseen causes of loss. As exposures evolve, the lack of understanding around silent cyber risks could pose a material threat to (re)insurers' future solvency."

While there is an increased number of takers for cyber insurance, the underwriters are concerned over the unquantified cyber coverage (like the incident of PF Chang's). The report points out the need for, "greater certainty, expertise, capacity and stability from the (re)insurance

market in a complex and growing risk area." It also notes that the "standalone insurance market holds the promise of unlocking the potential for meaningful coverage for both insurers and buyers." This means that traditional insurance companies' longstanding history in the insurance business could actually be holding them back from offering the solutions that an industry as dynamic as information security really needs. The structures they have in place may not apply to cybersecurity because threats are often unforeseeable, the impacts of known threats aren't easy to predict, and there is so much ongoing change that long-term policies can be out of date long before they expire. 🔒



GLOBAL 
CYBERLYMPICS

WORLD FINALS

THE HAGUE, NETHERLANDS

GAME OVER

09.26.2017

www.cyberlympics.org



SUBSCRIBE NOW

FOR COMPLETE ISSUE

TIM FITZGERALD